STRATEGIC STUDIES QUARTERLY

# Structural Causes and Cyber Effects

## A Response to Our Critics

*James Wood Forsyth Jr.*
*Maj Billy E. Pope, USAF*

**Abstract**

Evidence of the emerging cyber regime is mounting every day. Increasingly, states are bringing notoriously secretive cyber issues into the realm of public debate, particularly in response to events that threaten the availability, security, and surety of cyberspace. This is not to say sovereign states have taken to playing international politics with all of their cards on the table. States will continue to protect sensitive sources and methods as they always have. However, such evidence does lend credence to the idea that even powerful states realize cooperation in cyberspace is part of the domain itself. Furthermore, nonstate actors' attempts to influence state policy, atop the relatively anonymous platforms cyberspace offers, provide even more reason for states to cooperate in their attempts to shape and influence the information environment.

* * * * *

Three things came to mind when writing "Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace." First, we set out to provide an optimistic response to "cyber-pessimism." Second, we sought to conceptualize the domain within the thicker pattern of international politics. And third, we wanted to stimulate debate

---

Dr. James Wood Forsyth Jr. currently serves as professor of national security studies, USAF School of Advanced Air and Space Studies (SAASS), Maxwell AFB, Alabama. He earned his PhD at the Josef Korbel School of International Studies, University of Denver. He has written on great-power war, intervention, and nuclear issues.

Maj Billy Pope, USAF, is a cyber-operations officer and commander of the 81st Communications Squadron. He holds a master of public administration degree from Harvard's Kennedy School of Government and a master of military strategy from SAASS and is a PhD candidate studying the ethics of cyberwarfare.

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **2015** | | **00-00-2015 to 00-00-2015** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Structural Causes and Cyber Effects: A Response to Our Critics** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**Air Force Research Institute (AFRI) ,Strategic Studies Quarterly (SSQ),155 N. Twining Street Building 693,Maxwell AFB,AL,36112** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES

14. ABSTRACT

**Evidence of the emerging cyber regime is mounting every day. Increasingly states are bringing notoriously secretive cyber issues into the realm of public debate, particularly in response to events that threaten the availability, security, and surety of cyberspace. This is not to say sovereign states have taken to playing international politics with all of their cards on the table. States will continue to protect sensitive sources and methods as they always have. However, such evidence does lend credence to the idea that even powerful states realize cooperation in cyberspace is part of the domain itself. Furthermore, nonstate actors??? attempts to influence state policy, atop the relatively anonymous platforms cyberspace offers, provide even more reason for states to cooperate in their attempts to shape and influence the information environment.**

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a REPORT | b ABSTRACT | c THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **Same as Report (SAR)** | **8** | |

regarding the prospects of achieving great-power cooperation in cyberspace. Judging from the quality of the responses received, we seem to have been successful on all three counts.

When considering "Structural Causes and Cyber Effects," Christopher Whyte offers two important critiques of our argument—both of which have to do with its deterministic nature. In the first instance, no one can predict with Newtonian fidelity whether states will continue to play the determining role in international politics that we ascribe to them. As Whyte points out, a new medievalism may be on the horizon whereby the international system will "experience a complexification of processes as state power erodes." In the second instance, contemporary notions regarding the distribution of power, which historically favor the return of multipolarity, might prove to be incorrect. Obviously, our theoretical orientation is not in line with such claims, but that does not mean we hold the truth. Theory is not about truth. If truth is the question, we are in the realm of law, not theory. Theories explain things, and Waltzian realism still explains a lot about a number of big, important things. For the purposes of this discussion, however, we will put theoretical orientations aside and focus on the empirical qualities of cyberspace we can all agree on: *the world and its citizenry are becoming increasingly dependent upon cyberspace and the strong connections the domain facilitates*.

Ordinary social and political functions like interstate travel and market economies have been refined and optimized using the time and distance advantages cyberspace affords. Airplanes taking off from Islamabad, Pakistan, are already booked fully with follow-on passengers traveling three connections and three countries away. When a cloud of volcanic ash fills the airspace above Iceland, causing diversions and delays, massive computing power using cyberspace as its workspace mitigates the delays and keeps the complex scheduling system accommodating such travel from crumbling. Transnational corporations draw manufacturing components and expendable resources from every corner of the world in finite quantities with minimal transit times. These complex arrangements produce the goods and services that make up world trade. Corporate operations have become so entrenched in cyberspace that their competitive margins, both domestically and internationally, are dependent upon the efficiencies achieved by instantaneous communication and situational awareness.[1]

What does this have to do with international order and cyberspace? Quite simply, as traditional political and social functions become dependent upon cyberspace, states—both big and small—will have to pay attention to the domain in all its facets. These same states, as well as transnational actors, motivated by nothing more than selfish self-interest will accrue benefits from a cyberspace that is both accessible and wide-reaching. Competitive great powers, like large firms in an oligopolistic market—be there one, two, or more—can ill afford to live "off the grid" in the emerging information age; *yet living on the grid requires at least acquiescence to the structures and agencies that keep cyberspace alive*. This, coupled with protecting the enormous capital investments states and transnationals have made in things like undersea fiber-optic cables and associated high-tech infrastructures essential for cyberspace, makes the emergence of a cyber regime reasonable if not inevitable.

Moreover, as the world's information systems mature and increasing numbers of international actors face the critical intersection of dependency and vulnerability, it is fair to ask why cyberspace remains an ungoverned frontier today. Quite simply, regimes and the agreed norms they rest on take time. One look at the chronological development of early maritime standards provides a useful analogy. The sea laws of Oléron, first codified in the middle of the thirteenth century, for example, postdated man's dependence on the areas beyond the littorals by hundreds of years.[2] "Structural Causes and Cyber Effects" highlights the nuclear nonproliferation treaty as another example of how important, difficult agreements take time to unfold. Maturation of the domain will force hard questions into the realm of public debate and policy.

One important conundrum that surfaces repeatedly throughout the budding cyber-policy debate is the ability (or inability) to attribute cyber disruptions to their true sources. It is easy for actors in cyberspace today to remain anonymous if they choose to do so. Encryption technologies allow even unsophisticated actors to cover their tracks relatively well.[3] Nation-states and well-resourced nonstate actors have even more advanced capabilities that allow them to remain anonymous online.[4] These factors, coupled with the monetary and computing resources required to record the actions of individual people in cyberspace, make attribution a difficult task.

States must attenuate the attribution problem if they are to foster responsible behavior and accountability in cyberspace. Here again, the

most potent long-term solution to a thorny cyber-political issue rests in the need for cooperation. Attribution depends on evidence, and this evidence can be spread across information systems owned by several sovereign entities—be they states, commercial companies, or other politically motivated groups. Piecing this evidence together to pinpoint malefactors requires meticulous, coordinated transparency and information-sharing agreements.[5] While some evidence can be gleaned from publically available records and social media, states more often must work with one another to corroborate information into actionable intelligence. Furthermore, nonstate actors' attempts to influence state policy, atop the relatively anonymous platforms cyberspace offers, provide all the more reason for states to cooperate in their attempts to shape and influence the information environment.

Along these lines, Brian Mazanec raises important questions regarding our argument. His focus on norm development and technology is interesting but, in fairness, not a central concern of ours. As we put it,

> As the world transitions from unipolarity to multipolarity—as the structure of international politics changes—the collective dependencies upon the sea, air, space, *and* cyber will intensify. As dependencies intensify, the constraining effects produced by multipolarity and oligopolistic competition will be readily felt by all. . . . In such a world, the fortunes and security of each will be tightly coupled to the fortunes and security of the others, and as a result, the great powers will be incentivized to cooperate.[6]

In fact, there is little in Mazanec's rebuttal that disputes this. In large part, this is because, while we treat cyberspace as a domain, he treats it as a weapon. The two ideas are not mutually exclusive but do lead to different conclusions. Nevertheless, even when one considers cyberspace from the perspective of a weapon, his argument is not convincing. From our perspective, international agreements regarding nuclear, chemical, and biological weapons adequately explain why some states seek comfort from vulnerability through policy. Common sense tells us that when a state determines it is *vulnerable* to a weapon over which it holds little defense, it ought to strive to mitigate its vulnerabilities through any appropriate means necessary—policy being one. Not all states are this shrewd, but most of them are, most of the time. How else can one explain the longevity of the Non-Proliferation Treaty (NPT)? The NPT, although far from a perfect arrangement, has served as a defense for states too weak to build nuclear arsenals of their own; it has

lowered the risk of nuclear proliferation and has provided some stability in a world of 195 states where each is responsible for its own security. Why would cyberspace be any different? Given the inherent advantages of offense over defense, states today have little ability to defend themselves from attack.[7] This lends credence to the idea that nations will (or at least should) attempt to limit vulnerabilities through norms and policies where "hard" defenses cannot be put in place.

Moreover, evidence of the emerging cyber regime is mounting every day. Increasingly, states are bringing notoriously secretive cyber issues into the realm of public debate, particularly in response to events that threaten the availability, security, and surety of cyberspace. This is not to say sovereign states have taken to playing international politics with all of their cards on the table. States will continue to protect sensitive sources and methods as they always have. However, it does lend credence to the idea that even powerful states realize cooperation in cyberspace is part and parcel of the domain itself. One need only examine recent headlines to find such evidence.

The 2014 incident in which hackers compromised information systems at Sony Pictures Entertainment serves to illustrate this point. Hackers stole and damaged hundreds of gigabytes of data, including future movie scripts, internal financial documents, and employee records, in response to Sony's controversial film, *The Interview*. The United States Federal Bureau of Investigation publically implicated the North Korean government in the incident, saying "North Korea's attack on [Sony] reaffirms that cyber threats pose one of the gravest national security dangers to the United States."[8] Pres. Barack Obama followed this public indictment stating the United States would seek a "proportional response" as part of a campaign to warn against future attacks.[9] The response the US government selected was not one of unilateral retaliation but rather was a structured call for coordination and cooperation intended to fortify emerging norms of acceptable behavior in cyberspace. Secretary of State John Kerry articulated the US stance, saying, "This provocative and unprecedented attack and subsequent threats only strengthen our resolve to continue to work with partners around the world to strengthen cybersecurity, promote norms of acceptable state behavior, uphold freedom of expression, and ensure that the Internet remains open, interoperable, secure and reliable."[10]

Make no mistake, cooperation and compromise in cyberspace will not come easily, especially between states with competing interests. In fact, the United States openly requested assistance from China in response to the Sony incident—only to be given the diplomatic brush-off. The *New York Times* quoted one US official as saying "What we are looking for is a blocking action, something that would cripple [North Korea's] efforts to carry out attacks."[11] China responded by questioning the United States' evidence implicating the North Korean government in the first place.[12] This request from the United States came during a tense lapse in negotiations between the United States and China over America's open indictment of five Chinese military hackers for purported breaches into US government and commercial information systems.[13] Yet, each retreat from the negotiating table thus far has been matched by a subsequent overture for cooperation from both sides.

The United States and China have engaged in a public dialogue regarding the future of cyberspace, cyberwarfare, intelligence, and intellectual property since at least March 2013, when US National Security Advisor Tom Donilon overtly connected China with cyber activities against US interests.[14] This dialogue led to the establishment of an official bilateral US-China cyber working group that made progress toward "international cyberspace rules, and measures to boost dialogue and cooperation on cyber security."[15] However, suggestions that both the United States and China were engaged in cyber activities that threatened cooperation seemed to undermine and complicate these efforts.[16] Even amid pitted difficulties, both the United States and China acknowledge the value of cooperation and understanding to the continued potential of cyberspace. As recent as February 2015, J. Michael Daniel, special assistant to the president and cybersecurity coordinator at the National Security Council, wrote, "Our Chinese counterparts have told us that the United States and China should work together to build a more open, secure, interoperable and reliable cyberspace. We couldn't agree more."[17] In short, China's recent activities lend credence to the idea that it appears to be more interested in becoming a "norm maker" than a "norm breaker."

The United States and China are far from being the only stakeholders in the cyberspace-partnership debate. Since we published "Structural Causes and Cyber Effects," six members of the Shanghai Cooperation Organization (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan) partnered to present an updated code of conduct for cyber-

space to the United Nations (UN) general assembly in January 2015.[18] Additionally, the UN's International Telecommunications Union has increasingly focused on partnerships to extend the breadth and depth of cyberspace as a mainstay of traditional societal structures. The World Summit on the Information Society, for example, will gather a conglomerate of UN and UN Educational, Scientific, and Cultural Organization participants in May 2015 to focus on extending Internet and communications technologies to disadvantaged areas of the world.[19] Furthermore, the World Economic Forum and the government of Japan have partnered to host a multistakeholder dialogue on cybersecurity and the future of the Internet in November 2015. This summit, promising a cross-sectorial approach consisting of academic, governmental, and industry leaders is focused on "technology, policy-making and the development of cooperative standards and norms."[20]

The question for all interested parties to consider is: How does one explain all this activity in cyberspace? We have offered a structural explanation. That is to say, cyberspace cannot be comprehended as a separate realm of activity divorced from the context of international politics. Like other domains, order within cyberspace is contingent upon international order writ large. Thus, the great powers cannot choose to ignore cyberspace any more than they can choose to ignore the land, sea, air, or space. As the distribution of power throughout the world changes, the great powers will strive to create rules, norms, and standards of behavior that will mitigate the challenges posed by cyberspace—even if they might prefer not to. This does not mean they will be successful in their endeavors. It simply means states, acting in anarchy, have no other promising options. SSQ

**Notes**

1. Peter Dicken, *Global Shift: Mapping the Changing Contours of the World Economy*, 6th ed. (New York: Guilford Press, 2011), 81.

2. Charles H. Stockton, *The Codification of the Laws of Naval Warfare*, Proceedings of the American Society of International Law at Its Annual Meeting at George Washington University, 6 (25–27 April 1912), 116, http://www.jstor.org/stable/25656440.

3. Dan Goodin, "Scientists Detect 'Spoiled Onions' Trying to Sabotage Tor Privacy Network," *Ars Technica*, 21 January 2014, http://arstechnica.com/security/2014/01/scientists-detect-spoiled-onions-trying-to-sabotage-tor-privacy-network/. Tor is a widely available software client that allows anyone with a computer to traverse cyberspace anonymously using commercial-class encryption.

4. Eric F. Mejia, "Act and Actor Attribution in Cyberspace," *Strategic Studies Quarterly* 8, no. 1 (Spring 2014), 119.

5. P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2014), 73.

6. James Wood Forsyth Jr. and Billy E. Pope, "Structural Causes and Cyber Effects: Why International Order Is Inevitable in Cyberspace," *Strategic Studies Quarterly* 8, no. 4 (Winter 2014), 120–21.

7. Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Forces Quarterly* 61, no. 2 (2011): 10–17.

8. Federal Bureau of Investigation, "Update on Sony Investigation," 19 December 2014, http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

9. David E. Sanger, Nicole Perlroth, and Eric Schmitt, "U.S. Asks China to Help Rein In Korean Hackers," *New York Times*, 20 December 2014, http://www.nytimes.com/2014/12/21/world/asia/us-asks-china-to-help-rein-in-korean-hackers.html.

10. John Kerry, "Condemning Cyber-Attack by North Korea" (press release, Department of State, 19 December 2014), http://www.state.gov/secretary/remarks/2014/12/235444.htm.

11. Sanger, Perlroth, and Schmitt, "U.S. Asks China to Help Rein In Korean Hackers."

12. Hua Chunying, "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on December 22, 2014" (press release, Ministry of Foreign Affairs, People's Republic of China, 22 December 2014), http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1221668.shtml.

13. Ellen Nakashima, "Indictment of PLA Hackers Is Part of Broad U.S. Strategy to Curb Chinese Cyberspying," *Washington Post*, 22 May 2014, http://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html.

14. Tom Donilon, "Remarks By Tom Donilon, National Security Advisor to the President: 'The United States and the Asia-Pacific in 2013,' " (press release, Office of the Press Secretary, White House, 11 March 2013), https://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

15. Ben Blanchard, "China, U.S. Talks on Cyber Security Go Well: Xinhua," *Reuters*, 10 July 2013, http://www.reuters.com/article/2013/07/10/us-china-usa-cyber-idUSBRE96904820130710.

16. China continues to condemn revelations released by Edward Snowden that suggest the United States is engaged in cyber activities targeting Chinese information systems, and the United States continues to blame the Chinese government for intellectual property theft, particularly against American commercial companies.

17. J. Michael Daniel, Robert Holleyman, and Alex Niejelow, "China's Undermining an Open Internet," *POLITICO Magazine*, 4 February 2015, http://www.politico.com/magazine/story/2015/02/china-cybersecurity-114875.html.

18. Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations Addressed to the United Nations Secretary-General, letter, A/69/723, 9 January 2015, https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf.

19. "WSIS Forum 2015: Innovating Together: Enabling ICTs for Sustainable Development," WSIS Forum 2015 (web site), no date, http://www.itu.int/net4/wsis/forum/2015/.

20. Fon Mathuros, "Japan and World Economic Forum to Jointly Address Cybersecurity" (press release, World Economic Forum, 24 January 2015), http://www.weforum.org/news/japan-and-world-economic-forum-jointly-address-cybersecurity.

## Disclaimer